45495

BRAINWARE UNIVERSITY

Term End Examination 2025-2026
Programme – M.Sc.(ANCS)-2025
Course Name – API Penetration Testing
Course Code - MNC27504 (T)
(Semester II)

Full Marks : 40 **Time : 2:0 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 10=10

1. *Choose the correct alternative from the following :*

(i) Identify the primary role of an API in a microservices architecture.
   a) User interface rendering b) Service-to-service communication
   c) Database replication d) Operating system scheduling

(ii) Give examples the correct HTTP method semantics when deleting a resource via API.
   a) GET b) POST
   c) PATCH d) DELETE

(iii) Identify the role of API gateways in security enforcement.
   a) Replace backend services b) Centralize authentication and rate limiting
   c) Store user data d) Compile API code

(iv) Identify the primary purpose of authorization in API-driven systems.
   a) To verify user identity b) To control permitted actions on resources
   c) To encrypt API traffic d) To log user activity

(v) Identify the relationship between authentication and authorization.
   a) Authentication precedes authorization b) Authorization precedes authentication
   c) They are independent processes d) Authorization replaces authentication

(vi) Estimate the security impact of accepting expired JWTs in production APIs.
   a) Temporary service disruption b) Minor logging issues
   c) Unauthorized persistent access d) Improved availability

(vii) Choose the most reliable indicator of a distributed brute-force attack on APIs.
   a) Low-volume failures across many IPs b) Malformed JSON payloads
   c) Expired TLS certificates d) Single IP with high traffic

(viii) Choose the condition that makes GET requests particularly dangerous in CSRF scenarios.
   a) They can trigger state changes automatically b) They require authentication headers
   c) They disable cookies d) They support encryption

(ix) Identify the core trust failure that enables HTTP Host Header attacks.

a) Trusting client-supplied Host values
b) Broken access control
c) Weak encryption
d) Missing authentication

(x) Choose the most critical indicator of active SSTI exploitation during testing.

a) Expired cookies
b) Unexpected arithmetic evaluation in templates
c) Slow response time
d) Static HTML output

Group-B

(Short Answer Type Questions) 3 x 5=15

2. Differentiate between public, partner, and internal APIs with respect to attack surface and risk. (3)
3. Describe the conceptual difference between authentication and authorization with reference to API security. (3)
4. Differentiate between object-level and function-level authorization in APIs with suitable context. (3)
5. Evaluate the security risks introduced by exposing internal fields in authenticated API responses. (3)
6. Evaluate the security impact of Broken Function Level Authorization in administrative API endpoints. (3)

OR

Justify a secure authorization strategy suitable for microservices-based API architectures. (3)

Group-C

(Long Answer Type Questions) 5 x 3=15

7. Explain the concept of SQL Injection in API authentication mechanisms and discuss how it enables login bypass. (5)
8. Differentiate between Local File Inclusion and Remote File Inclusion based on exploitation method, configuration dependency, and impact. (5)
9. Assess the role of insecure frontend consumption of API responses in the emergence of XSS vulnerabilities. (5)

OR

Critique the effectiveness of traditional input validation techniques in preventing context-based XSS attacks. (5)

****